

Appl. No. : **09/818,699**
Filed : **March 27, 2001**

AMENDMENTS TO THE CLAIMS

Please amend Claims 1, 5, 7, 8, 12, and 20-24 as indicated below.

1. (Currently Amended) A method of transferring data over a computer network from a network server to a client computer system, the method comprising:

receiving a request by a requestor using a first client computer system for data from at least one network server storing data, at least some of the data stored by the network server being encrypted;

checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key;

if the requested data is encrypted with the encryption key, sending the encrypted data to the first client computer system ~~without an associated decryption key~~;

sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor;

if the requested data is unencrypted, automatically retrieving the encryption key associated with the requestor from the first client computer system and;

encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data; and

sending the encrypted data to the first client computer system ~~without the associated decryption key~~ wherein the client computer system uniquely retains a private key uniquely associated with the client computer system such that other client systems do not have access to the private key and wherein both the encryption key and the private key are needed for decryption of encrypted data.

2.-4. (Canceled)

Appl. No. : 09/818,699
Filed : March 27, 2001

5. (Currently Amended) A method of data storage and retrieval comprising:
- automatically generating independently of information from a network server a public encryption key and a corresponding private encryption key in a client computer system, wherein the network server stores at least some data in an encrypted format and wherein the private encryption key is uniquely associated with the client computer,
 - storing the public encryption key and the corresponding private encryption key in the client computer system such that access to the private encryption key is limited solely to the client computer and wherein both the public and the private encryption keys are needed to decrypt encrypted data;
 - associating an attribute with a data file, the attribute indicating whether the data file is encrypted with the public encryption key when stored on the network server, and the attribute indicating an owner of the public encryption key;
 - requesting the data file by a requestor from the network server using the client computer system;
 - sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor;
 - checking the attribute of the requested data file to determine whether the requested data file is encrypted;
 - if the requested data file is encrypted with the requestor's key, forwarding the requested data file to the client computer system ~~without the requestor's encryption key~~ and;
 - if the requested data file is unencrypted, sending the public encryption key from the client computer system to the network server automatically and without user intervention;
 - forwarding the requested data file to the client computer system after the public encryption key is used to encrypt the requested data file to create an encrypted data file wherein the encrypted data file is forwarded to the requestor ~~without the requestor's encryption key~~; and
 - storing the encrypted data file on a storage medium in the client computer system.

Appl. No. : 09/818,699
Filed : March 27, 2001

6. (Canceled)

7. (Currently Amended) The method of Claim 5, wherein at least one of the public encryption key and the corresponding private encryption key are based on a password entered by a user when logging on to the client computer system.

8. (Currently Amended) A computer readable data storage medium having stored thereon commands that are operative to cause a general purpose computer configured as a network server to perform a method of data retrieval comprising:

receiving a request for a data file from a requestor using a first client computer system at a network server, wherein at least some data files are encrypted;

checking a file attribute of the requested data file to determine whether the requested data file is encrypted with an encryption key associated with the requestor, wherein the attribute is alterable by a network administrator;

if the requested data file is encrypted with the encryption key associated with the requestor, routing the encrypted data file to the first client computer system ~~without the requestor's encryption key~~;

sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor and;

if the requested data file is unencrypted, automatically requesting ~~the~~ a public encryption key associated with the requestor from the first client computer system, the public encryption key being originated independently of the network server and wherein the client computer system retains a private decryption key that is unique to the client computer system;

automatically encrypting the requested data file using the public encryption key associated with the requestor to create an encrypted data file; and

routing the encrypted data file to the first client computer system such that other client computer systems do not have access to the private decryption key associated with the first client computer system without the requestor's encryption key.

9. (Canceled)

10. (Canceled)

Appl. No. : **09/818,699**
Filed : **March 27, 2001**

11. (Cancelled)
12. (Currently Amended) The method of Claim 1, further comprising sending the requested data to the first client computer system only if the requested data is encrypted and if the requestor is the owner of the encryption key.
13. (Previously Presented) The method of Claim 1, wherein the encryption key is derived at least in part from an identification code.
14. (Previously Presented) The method of Claim 13, wherein the encryption key is derived at least in part from user input.
15. (Canceled)
16. (Canceled)
17. (Previously Presented) The method of Claim 5, further comprising sending the requested data file to the client computer system if the requested data file is encrypted and the requestor is the owner of the public encryption key.
18. (Canceled)
19. (Canceled)
20. (Currently Amended) The data storage medium of Claim 8, further comprising sending the requested data file to the first client computer system if the requested data file is encrypted and the requestor is the owner of the encryption key.
21. (Currently Amended) The computer readable data storage medium of Claim 8, wherein the encryption key is based at least partially on data associated with the first client computer system.
22. (Currently Amended) The computer readable data storage medium of Claim 21, wherein the data associated with the first client computer system is uniquely associated with the client computer system.
23. (Currently Amended) The computer readable data storage medium of Claim 21, wherein the encryption key is also based on user input provided to the first client computer system.
24. (Currently Amended) The method of Claim 13, wherein the identification code is uniquely associated with the first client computer system.